CLAIMS

What is claimed is:

1. A method of secure key exchange between a first entity and a second entity comprising:

generating, by the first entity, a first key, encrypting the first key with a public key of a third entity, and storing the encrypted first key in the third entity;

generating, by the second entity, a second key, encrypting the second key with the public key of the third entity, and storing the encrypted second key in the third entity;

decrypting, by the third entity, the encrypted first key and the encrypted second key, using the third entity's private key to obtain the first key and the second key;

encrypting, by the third entity, the first key using the second key, and storing the first key encrypted by the second key in the third entity;

obtaining, by the second entity, the first key encrypted by the second key, and decrypting, using the second key, the first key encrypted by the second key.

2. The method of claim 1, further comprising encrypting content with the first key by the second entity and transferring the encrypted content from the second entity to the first entity.

3. The method of claim 1, wherein the first entity comprises a graphics device.

4. The method of claim 1, wherein the second entity comprises an application program.

5. The method of claim 1, wherein the third entity comprises a trusted platform module.

6. The method of claim 1, wherein generating the first key comprises pseudorandomly generating the first key, and generating the second key comprises pseudorandomly generating the second key.

7. The method of claim 1, wherein the first key and the second key comprise symmetric keys.

8. The method of claim 1, further comprising signaling the first entity, by the second entity, to start the key exchange.

9. The method of claim 8, wherein signaling comprises storing a value in a register resident in the first entity.

10. A system for secure key exchange comprising:

a third entity having a public/private key pair;

a first entity to generate a first key, to encrypt the first key with the public key of the third entity, and to store the encrypted first key in the third entity;

a second entity to generate a second key, to encrypt the second key with the public key of the third entity, and to store the encrypted second key in the third entity;

wherein the third entity decrypts the encrypted first key and the encrypted second key using the third entity's private key to obtain the first key and the second key, encrypts the first key using the second key, and stores the first key encrypted by the second key in the third entity; and

wherein the second entity obtains the first key encrypted by the second key from the third entity, and decrypts, using the second key, the first key encrypted by the second key.

11. The system of claim 10, wherein the first entity comprises a graphics device.

12. The system of claim 10, wherein the second entity comprises an application program.

13. The system of claim 10, wherein the third entity comprises a trusted platform module.

14. The system of claim 13, wherein the trusted platform module comprises a first register to store the encrypted first key, a second register to store the encrypted second key, and a third register to store the first key encrypted by the second key.

15. The system of claim 10, wherein the first key and the second key comprise pseudorandomly generated symmetric keys.

16. The system of claim 10, wherein the second entity encrypts content with the first key and transfers the encrypted content to the first device.

17. The system of claim 10, wherein the third entity comprises an input/output pin dedicated for use by the first entity, and the first entity is coupled to the dedicated input/output pin using a buried line on a printed circuit board.

18. A method of secure key exchange and protected content distribution between a graphics device and an application program comprising:

pseudorandomly generating, by the graphics device, a first symmetric key, encrypting the first symmetric key with a public key of a trusted platform module (TPM), and storing the encrypted first symmetric key in a first register in the TPM;

pseudorandomly generating, by the application program, a second symmetric key, encrypting the second symmetric key with the public key of the

TPM, and storing the encrypted second symmetric key in a second register in the TPM;

decrypting, by the TPM, the encrypted first symmetric key and the encrypted second symmetric key using the TPM's private key to obtain the first symmetric key and the second symmetric key;

encrypting, by the TPM, the first symmetric key using the second symmetric key, and storing the first symmetric key encrypted by the second symmetric key in a third register in the TPM;

obtaining, by the application program, the first symmetric key encrypted by the second symmetric key from the third register, and decrypting, using the second symmetric key, the first symmetric key encrypted by the second symmetric key; and

encrypting content, by the application program, using the first symmetric key, and sending the encrypted content to the graphics device.

19. The method of claim 18, further comprising signaling the graphics device, by the application program, to start the key exchange.

20. The method of claim 19, wherein signaling comprises storing a value in a register resident in the graphics device.

21. The method of claim 18, further comprising, decrypting, by the graphics device, the encrypted content using the first symmetric key.